PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-324418
(43)Date of publication of application : 14.11.2003

(51)Int.Cl. H04L 9/08
H04L 9/14
H04N 7/167

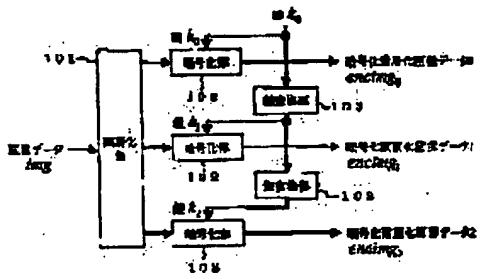
(21)Application number : 2002-157553
(22)Date of filing : 30.05.2002

(71)Applicant : CANON INC
(72)Inventor : TAGASHIRA NOBUHIRO
SUGA YUJI
HAYASHI JUNICHI
IWAMURA KEIICHI

(30)Priority
Priority number : 2002051823 Priority date : 27.02.2002 Priority country : JP

(54) IMAGE PROCESSOR, DATA PROCESS APPARATUS AND METHOD THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To easily manage a key when enciphering data in each hierarchy by using a key for each hierarchy.
SOLUTION: The image processor has a key conversion part (103) for generating a key different for each hierarchy based upon a specific key with respect to image data having a hierarchical structure and an enciphering part (102) for enciphering image data in a prescribed hierarchy by using the key for each hierarchy.



LEGAL STATUS
[Date of request for examination] 30.05.2005
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's

decision of rejection]
[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2003－324418
(P2003－324418A)
(43)公開日　平成15年11月14日(2003.11.14)

(51)Int.Cl.'		識別記号	FI		テーマコード'(参考)	
H04L	9/08		H04L	9/00	601A	5C064
	9/14				641	5J104
H04N	7/167		H04N	7/167	Z	

審査請求　未請求　請求項の数25　ＯＬ　（全 14 頁）

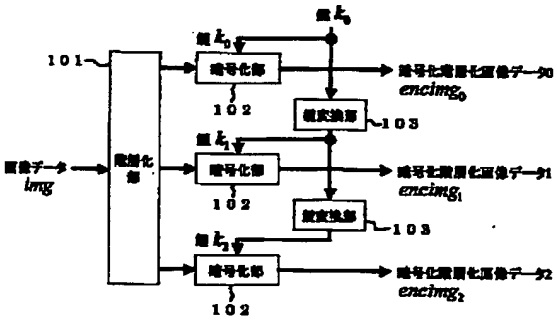
(21)出願番号　特願2002－157553(P2002－157553)
(22)出願日　平成14年５月30日(2002.5.30)
(31)優先権主張番号　特願2002－51823(P2002－51823)
(32)優先日　平成14年２月27日(2002.2.27)
(33)優先権主張国　日本（ＪＰ）

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　田頭　信博
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(72)発明者　須賀　祐治
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　100090273
弁理士　國分　孝悦

最終頁に続く

(54)【発明の名称】　画像処理装置、データ処理装置及びデータ処理方法

(57)【要約】
【課題】　各階層毎のデータに対して各階層毎の鍵を用いて暗号化する際に、鍵の管理を容易に行うことを課題とする。
【解決手段】　階層構造をもつ画像データに対して、特定の鍵を基に各階層毎に異なる鍵を生成する鍵変換手段（１０３）と、階層毎の鍵を用いて所定の階層の画像データを暗号化する暗号化手段（１０２）とを有することを特徴とする画像処理装置が提供される。



1

【特許請求の範囲】

【請求項１】　階層構造をもつ画像データに対して、特定の鍵を基に各階層毎に異なる鍵を生成する鍵変換手段と、前記階層毎の鍵を用いて所定の階層の画像データを暗号化する暗号化手段とを有することを特徴とする画像処理装置。

【請求項２】　前記暗号化手段は、前記階層毎の鍵のうちの１つの鍵を暗号化し、前記暗号化された各階層の画像データと共に出力する請求項１記載の画像処理装置。

【請求項３】　階層構造をもつ画像データが各階層毎に異なる鍵で暗号化されている画像データに対して、特定の鍵を基に各階層毎に異なる鍵を生成する鍵変換手段と、前記階層毎の鍵を用いて所定の階層の画像データを復号する復号手段とを有することを特徴とする画像処理装置。

【請求項４】　前記特定の鍵は、自己の階層に隣接する階層の変換に用いる鍵であって、前記鍵変換手段は、一方向性関数を用いて鍵を生成することを特徴とする請求項１～３のいずれか１項に記載の画像処理装置。

【請求項５】　階層構造をもつ画像データが各階層毎に異なる鍵で暗号化されている画像データに対して、ある鍵を用いて該鍵の階層に対応する階層及びその階層以下の階層の画像データを復号する復号手段を有することを特徴とする画像処理装置。

【請求項６】　階層構造をもつ画像データが各階層毎に異なる鍵で暗号化されている画像データ及び該階層毎の鍵のうちの１つの鍵が暗号化されている暗号化鍵に対して、前記暗号化鍵を復号し、該復号した鍵を用いて該鍵の階層に対応する階層及びその階層以下の階層の画像データを復号する復号手段とを有することを特徴とする画像処理装置。

【請求項７】　前記復号手段は、前記鍵を一方向性関数によって変換することにより、隣接する階層の画像データの復号に用いる鍵を生成することを特徴とする請求項５または請求項６に記載の画像処理装置。

【請求項８】　前記暗号化鍵の暗号化方式は、秘密鍵暗号アルゴリズムであることを特徴とする請求項２または請求項６に記載の画像処理装置。

【請求項９】　前記暗号化鍵の暗号化方式は、公開鍵暗号アルゴリズムであることを特徴とする請求項２または請求項６に記載の画像処理装置。

【請求項１０】　最上位階層の画像データの暗号化又は復号に用いる鍵は、特定の秘密情報に依存する情報であることを特徴とする請求項１～９のいずれか１項に記載の画像処理装置。

【請求項１１】　最上位階層の画像データの暗号化又は復号に用いる鍵は、画像データに依存する情報であることを特徴とする請求項１～９のいずれか１項に記載の画像処理装置。

【請求項１２】　最上位階層の画像データの暗号化又は

2

復号に用いる鍵は、特定の秘密情報及び画像データに依存する情報であることを特徴とする請求項１～９のいずれか１項に記載の画像処理装置。

【請求項１３】　前記階層構造は解像度に基づいた階層構造であって、上位階層になるにつれて解像度が高くなることを特徴とする請求項１～１２のいずれか１項に記載の画像処理装置。

【請求項１４】　前記階層構造は画像の重要度に基づいた階層構造であって、上位階層になるにつれて重要度が高くなることを特徴とする請求項１～１２のいずれか１項に記載の画像処理装置。

【請求項１５】　階層的な構造はSNRに基づいた階層構造であって、上位階層になるにつれてSNRが低くなることを特徴とする請求項１～１２のいずれか１項に記載の画像処理装置。

【請求項１６】　階層構造をもつマルチメディアデータに対して、特定の鍵を基に各階層毎に異なる鍵を生成する鍵変換手段と、前記階層毎の鍵を用いて所定の階層のマルチメディアデータを暗号化する暗号化手段とを有することを特徴とするデータ処理装置。

【請求項１７】　前記暗号化手段は、前記階層毎の鍵のうちの１つの鍵を暗号化し、前記暗号化された各階層のマルチメディアデータと共に出力する請求項１６記載のデータ処理装置。

【請求項１８】　階層構造をもつマルチメディアデータが各階層毎に異なる鍵で暗号化されているマルチメディアデータに対して、特定の鍵を基に各階層毎に異なる鍵を生成する鍵変換手段と、前記階層毎の鍵を用いて所定の階層のマルチメディアデータを復号する復号手段とを有することを特徴とするデータ処理装置。

【請求項１９】　前記特定の鍵は、自己の階層に隣接する階層の変換に用いる鍵であって、前記鍵変換手段は、一方向性関数を用いて鍵を生成することを特徴とする請求項１６～１８のいずれか１項に記載のデータ処理装置。

【請求項２０】　階層構造をもつマルチメディアデータが各階層毎に異なる鍵で暗号化されているマルチメディアデータに対して、ある鍵を用いて該鍵の階層に対応する階層及びその階層以下の階層のマルチメディアデータを復号する復号手段を有することを特徴とするデータ処理装置。

【請求項２１】　階層構造をもつマルチメディアデータが各階層毎に異なる鍵で暗号化されているマルチメディアデータ及び及び該階層毎の鍵のうちの１つの鍵を暗号化されている暗号化鍵に対して、　前記暗号化鍵を復号し、該復号した鍵を用いて該鍵の階層に対応する階層及びその階層以下の階層のマルチメディアデータを復号する復号手段とを有することを特徴とするデータ処理装置。

【請求項２２】　前記復号手段は、前記鍵を一方向性関

数によって変換することにより、隣接する階層のマルチメディアデータの復号に用いる鍵を生成することを特徴とする請求項２０または請求項２１に記載のデータ処理装置。

【請求項２３】　階層構造をもつマルチメディアデータに対して、特定の鍵を基に各階層毎に異なる鍵を生成する鍵変換ステップと、前記階層毎の鍵を用いて所定の階層のマルチメディアデータを暗号化する暗号化ステップとを有することを特徴とするデータ処理方法。

【請求項２４】　階層構造をもつマルチメディアデータが各階層毎に異なる鍵で暗号化されているマルチメディアデータに対して、ある鍵を用いて該鍵の階特定の鍵を基に各階層毎に異なる鍵を生成する鍵変換ステップと、前記階層毎の鍵を用いて所定の階層のマルチメディアデータを復号する復号ステップとを有することを特徴とするデータ処理方法。

【請求項２５】　階層構造をもつマルチメディアデータが各階層毎に異なる鍵で暗号化されているマルチメディアデータに対して、ある鍵を用いて該鍵の階層に対応する階層及びその階層以下の階層のマルチメディアデータを復号する復号ステップを有することを特徴とするデータ処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、データ処理に関し、特に、階層構造のデータの暗号化技術に関する。

【０００２】

【従来の技術】近年、パーソナルコンピュータ、PDA、携帯電話等、さまざまなデジタル機器が開発され、用いられるようになってきた。これらのデジタル機器は、画像表示に関して、画面の大きさ、または解像度、色数等、種々の機能を有する。これらの表示機能の多機能化に対応するように、画像フォーマットも様々なものが存在する。特に、フラッシュピクス、JPEG2000 にように、画像を階層的に有するフォーマットがある。これらの階層的な構造を持つファーマットのいくつかは、階層化画像データとして隣接する階層化画像データとの差分データだけを保持することにより、画像データ量を削減している。

【０００３】　一方、デジタル機器の高性能化による自由なデジタルコンテンツの利用とデジタルコンテンツの品質の向上により、デジタルコンテンツの著作権保護が問題視されるようになってきた。

【０００４】このような背景の下、階層的な画像に関して、階層毎のアクセス制御を実現するさまざまな発明が行われてきた。

【０００５】特開平 6-301754 は、少なくとも一つ以上の低解像度画像と少なくとも一つ以上の高解像度画像からなるデジタル画像を記憶した記憶媒体であって、低解像度画像は鍵を使用することなくアクセス可能であり、

高解像度画像は鍵を用いてのみアクセス可能であることを特徴とする記憶媒体とある。画像を低解像度画像と高解像度画像に分解し、高解像度画像に対して鍵を用いて暗号化を行うことにより、この機能を実現している。

【０００６】また、特許第 2606074 号は、画像データを複数の空間成分に分解し、各成分毎に符号化し、各符号化データ毎に暗号化し、暗号化データを多重化する画像符号化装置を送信側に備え、多重化データを分離し、分離した各データを暗号化に対する復号し、各暗号に対する復号データを符号化に対する復号し、各成分データから画像データを合成する画像復号装置を受信側に備えることを特徴とする画像暗号化伝送方式である。

【０００７】

【発明が解決しようとする課題】特許第 2606074 号は、暗号化の鍵の管理に関する記述はなく、鍵の管理方法は不明である。

【０００８】また、特開平 6-301754 は、暗号化の鍵はユーザ入力と書かれている。画像の各階層毎のアクセス制御を実現することを目的であることを考えると、各階層の暗号化に用いられている鍵を同じ鍵とすることはできない。さらに、階層化画像データが隣接する階層化画像データとの差分データである場合であって、特定の階層化画像データにアクセスしようとする場合、アクセスしようとしている階層化画像データに対応する鍵だけでなく、依存する階層化画像データに対応する全ての鍵も必要となる。これに対して、特開平 6-301754 は、低階層の画像データである低解像度画像データは暗号化しないとしている。しかし、この方法では、画像データの全てに対してアクセス制御を行いたいという要求に答えることができない。

【０００９】また、近年のデジタル機器の高機能化による画像の品質の向上により、画像の高解像度側の上限はどんどん高くなっている。一方、携帯電話、PDA 等のモバイル機器における画像の利用を考えると低解像度側の下限は低くなることはなくても、大幅に高くなることはない。このことは、画像の解像度の幅が広くなることを意味し、階層的な画像において、階層の数が多くなることを意味する。これに対して、従来の方式で鍵管理を行うと、階層が増える毎に管理すべき鍵が増大し、鍵の管理方法が問題となってくる。

【００１０】さらに、暗号化の鍵の管理を考えた場合、利用者の持つ鍵を利用すること等により、鍵の配送の問題を軽減したいという要求もある。

【００１１】本発明は、上記の実状をかんがみてなされたものであり、階層的なデータに対するアクセス制御において、アクセス制御に用いる鍵を削減し、鍵の管理を容易にする技術を提供することを目的とする。さらに、利用者への鍵の配送も容易にする技術を提供することを目的とする。

【００１２】

5

【課題を解決するための手段】本発明の一観点によれば、階層構造をもつ画像データに対して、特定の鍵を基に各階層毎に異なる鍵を生成する鍵変換手段と、前記階層毎の鍵を用いて所定の階層の画像データを暗号化する暗号化手段とを有することを特徴とする画像処理装置が提供される。本発明の他の観点によれば、階層構造をもつ画像データが各階層毎に異なる鍵で暗号化されている画像データに対して、特定の鍵を基に各階層毎に異なる鍵を生成する鍵変換手段と、前記階層毎の鍵を用いて所定の階層の画像データを復号する復号手段とを有することを特徴とする画像処理装置が提供される。本発明のさらに他の観点によれば、階層構造をもつ画像データが各階層毎に異なる鍵で暗号化されている画像データに対して、ある鍵を用いて該鍵の階層に対応する階層及びその階層以下の階層の画像データを復号する復号手段を有することを特徴とする画像処理装置が提供される。本発明のさらに他の観点によれば、階層構造をもつ画像データが各階層毎に異なる鍵で暗号化されている画像データ及び該階層毎の鍵のうちの1つの鍵が暗号化されている暗号化鍵に対して、前記暗号化鍵を復号し、該復号した鍵を用いて該鍵の階層に対応する階層及びその階層以下の階層の画像データを復号する復号手段とを有することを特徴とする画像処理装置が提供される。本発明のさらに他の観点によれば、階層構造をもつマルチメディアデータに対して、特定の鍵を基に各階層毎に異なる鍵を生成する鍵変換手段と、前記階層毎の鍵を用いて所定の階層のマルチメディアデータを暗号化する暗号化手段とを有することを特徴とするデータ処理装置が提供される。本発明のさらに他の観点によれば、階層構造をもつマルチメディアデータが各階層毎に異なる鍵で暗号化されているマルチメディアデータに対して、特定の鍵を基に各階層毎に異なる鍵を生成する鍵変換手段と、前記階層毎の鍵を用いて所定の階層のマルチメディアデータを復号する復号手段とを有することを特徴とするデータ処理装置が提供される。本発明のさらに他の観点によれば、階層構造をもつマルチメディアデータが各階層毎に異なる鍵で暗号化されているマルチメディアデータに対して、ある鍵を用いて該鍵の階層に対応する階層及びその階層以下の階層のマルチメディアデータを復号する復号手段を有することを特徴とするデータ処理装置が提供される。本発明のさらに他の観点によれば、階層構造をもつマルチメディアデータが各階層毎に異なる鍵で暗号化されているマルチメディアデータ及び及び該階層毎の鍵のうちの1つの鍵を暗号化されている暗号化鍵に対して、前記暗号化鍵を復号し、該復号した鍵を用いて該鍵の階層に対応する階層及びその階層以下の階層のマルチメディアデータを復号する復号手段とを有することを特徴とするデータ処理装置が提供される。本発明のさらに他の観点によれば、階層構造をもつマルチメディアデータに対して、特定の鍵を基に各階層毎に異なる鍵を生成する鍵変換ステップと、前記階層毎の鍵を用いて所定の階層のマルチメディアデータを暗号化する暗号化ステップとを有することを特徴とするデータ処理方法が提供される。本発明のさらに他の観点によれば、階層構造をもつマルチメディアデータが各階層毎に異なる鍵で暗号化されているマルチメディアデータに対して、ある鍵を用いて該鍵の階特定の鍵を基に各階層毎に異なる鍵を生成する鍵変換ステップと、前記階層毎の鍵を用いて所定の階層のマルチメディアデータを復号する復号ステップとを有することを特徴とするデータ処理方法が提供される。本発明のさらに他の観点によれば、階層構造をもつマルチメディアデータが各階層毎に異なる鍵で暗号化されているマルチメディアデータに対して、ある鍵を用いて該鍵の階層に対応する階層及びその階層以下の階層のマルチメディアデータを復号する復号ステップを有することを特徴とするデータ処理方法が提供される。

6

【００１３】本発明によれば、各階層毎のデータに対して各階層毎の鍵を用いて暗号化する際に、特定の鍵を基に各階層毎に異なる鍵を生成するので、鍵の管理を容易に行うことができる。また、暗号化されたデータと共に暗号化された鍵を利用者に供給することにより、利用者への鍵の配送も容易に行うことができる。

【００１４】

【発明の実施の形態】以下、本発明の実施の形態について図面を用いて説明する。図１は、本発明の実施の形態による画像アクセス制御装置（画像処理装置）の概要を示した構成図である。図１に示すように本実施の形態は、階層化部101と複数の暗号化部102と複数の鍵変換部103から構成される。

【００１５】階層化部101は、画像データimgを入力し、入力した画像データを階層毎に分離し、各階層化画像データを出力する。

【００１６】暗号化部102は、階層化画像データを入力し、鍵k0,k1,k2を用いて入力した階層化画像データを暗号化し、暗号化階層化画像データencimg0, encimg1, encimg2を出力する。ここで用いる暗号化アルゴリズムは、DES (Data Encryption Standard) や AES (Advanced Encryption Standard) 等暗号アルゴリズムが利用可能であるが、特に限定しない。

【００１７】鍵変換部103は、鍵k0を入力し、入力した鍵を変換し、鍵k1,k2を出力する。図2 に示すように、鍵変換部103は、一方向性関数で構成され、鍵の変換は一方向性関数を用いて変換される。一方向性関数とは、入力データを変換して出力データを求めることは簡単であるが、逆変換である出力データを逆変換して入力データを求めることが困難、もしくは不可能な関数である。

【００１８】一方向性関数の一つに、一方向性ハッシュ関数がある。一方向性ハッシュ関数H() は、異なる x1、x2 に対して H(x1)=H(x2) となる衝突が起こりにくい、任意の長さのデータをある長さのデータへ変換する

圧縮関数である。したがって、H(x1)=H(x2) を満たす x1、x2 を容易に見出すことが困難である。このとき、任意の y から y=H(x) となる x を容易に見出すことも困難となり、一方向性関数となる。これらの一方向性ハッシュ関数には、MD5 (Message Digest 5)、SHA-1(Secure Hash Algorithm 1) 等が知られている。

【００１９】さらに別の一方向性関数の一つに、暗号化関数を用いた方法がある。鍵 k を用いてデータ x を暗号化し、暗号化データ y を得る場合を y=Enc_k(x) と表す。ここで、入力データを x、出力データを y とし、出力データ y を次式 y=Enc_x(x) で求めることにより、一方向性関数を実現可能である。つまり、データ x を保持している場合は、鍵 x を知っているためにデータ x からデータ yを求めることが可能であるが、データ y だけを保持している場合は、鍵 x を知らないためにデータ y からデータ x を求めることが困難である。さらにまた、CBC (Cipher Block Chaining) 等の暗号化モードを利用することにより、任意の長さのデータをある長さのデータへ変換する圧縮関数を実現することも可能である。本実施の形態において、暗号化関数を用いた方法で一方向性関数を実現することは、画像データの暗号化に用いる暗号化関数と共用することを可能とし、実装時の回路やプログラムの小型化を実現する。ただし、本実施の形態は、一方向性関数を上記の関数に限定するものではない。

【００２０】以上のように、階層化部１０１は階層構造をもつ画像データを生成し、鍵変換部１０３は、特定の鍵kを基に各階層毎に異なる鍵を生成し、暗号化部１０２は各階層毎の画像データに対して前記各階層毎の鍵を用いて暗号化する。

【００２１】図３は、階層化画像データを暗号化する鍵と階層化画像データの対応を示した図である。以下は、画像の解像度に基づいて階層化画像データが構成されており、最高解像度の階層化画像データは最高階層化画像データであって、最低解像度の階層化画像データは最低階層化画像データであるとする。

【００２２】図３の左側に、階層化画像データを示す。階層化画像データは、img0 から img2 で表現され、階層化画像データ img0 が最高解像度の階層化画像データであって、階層化画像データ img2 が最低解像度の階層化画像データであるとする。

【００２３】図３の中央に、鍵を示す。最高解像度の階層化画像データの暗号化に用いる鍵を k0 とし、最低解像度の階層化画像データの暗号化に用いる鍵を k2 とする。また、一方向性関数を H() と表し、図３に示すように、一方向性関数 H()を用いて、鍵を順次変換する。

【００２４】図３の右側に、暗号化階層化画像データを示す。暗号化関数を Enc() と表し、添え字は鍵を表す。つまり、最高解像度の階層化画像データは、鍵 k0 を鍵として暗号化し、最低解像度の階層化画像データは、鍵 k2 を鍵として暗号化する。

【００２５】次に、図４を参照して、利用者毎の階層化画像データを含む画像ファイルフォーマットの一例を示す。図４に示すように、画像ファイルフォーマットは、暗号化画像データの部分とヘッダの部分に分けられ、暗号化階層化画像データの部分には階層化暗号化画像データencimg0～encimg2が含まれ、ヘッダの部分には鍵の暗号化データが含まれる。以下に、画像データが図３に示した３階層の階層化画像データである場合を想定し、説明する。

【００２６】利用者Ａは鍵kAを予め保持し、最高解像度の画像にアクセス可能な利用者とした場合の画像ファイルフォーマットを図４の左側に示す。暗号化画像データの部分は、暗号化階層化画像データencimg0とencimg1とencimg2を含み、また、ヘッダの部分は、鍵の暗号化データを含む。鍵の暗号化データは、利用者Ａの鍵kAを用いて、最高解像度の画像データにアクセスするための鍵k0を暗号化したデータである。

【００２７】また、利用者Ｂは鍵kBを予め保持し、最低解像度の画像にアクセス可能な利用者とした場合の画像ファイルフォーマットを図４の右側に示す。暗号化画像データの部分は、利用者Ａの暗号化画像データの部分と同様、暗号化階層化画像データencimg0とencimg1とencimg2を含み、また、ヘッダの部分は、鍵の暗号化データを含む。鍵の暗号化データは、利用者Ｂの鍵kBを用いて、最低解像度の画像データにアクセスするための鍵k2を暗号化したデータである。

【００２８】次に、図３を参照して、各階層化画像データにアクセスする場合を説明する。本実施の形態は、画像データのアクセス制御を実現するため方法であって、画像データの利用者は鍵を保持しているものとする。

【００２９】まず、最高解像度の画像データにアクセス可能な鍵 k0 を保持している利用者について説明する。鍵 k0 を保持している利用者は、鍵 k0 を用いて、暗号化階層化画像データ encimg0 を復号し、階層化画像データ img0 を得ることが可能である。さらに、一方向性関数を用いて、鍵 k0 から鍵 k1 を得ることも可能である。以下同様に、鍵 k1 を用いて、暗号化階層化画像データ encimg1 を復号し階層化画像データ img1 を得ることが可能であり、さらに、一方向性関数を用いて、鍵 k1 から鍵 k2 を得ることが可能である。さらに同様に、階層化画像データ img2 も得ることが可能になり、画像データを復元することが可能となる。

【００３０】次に、最低解像度の画像データにアクセス可能な鍵 k2 を保持している利用者について説明する。鍵 k2 を保持している利用者は、鍵 k2 を用いて、暗号化階層化画像データ encimg2 を復号し、階層化画像データ img2 を得ることが可能である。しかし、鍵の変換

9

は一方向性関数による変換なので、鍵 k2 から鍵 k1や鍵 k0 を得ることはできない。したがって、暗号化階層化画像データ encimg1や encimg0 を復号することもできず、階層化画像データ img1 や img0 を得ることができない。つまり、鍵 k2 を保持する利用者は、鍵 k2 に対応する階層化画像データとそれ以下の階層化画像データしか得ることができない。これは、サムネイル画像データの利用のように最低解像度の画像データである最低階層化画像データだけの自由なアクセスの実現を容易に可能にする。つまり、本実施の形態は、最低階層化画像データの暗号化に用いた鍵を常に公開することにより、だれでも最低階層化画像データにアクセス可能とする一方で、鍵の一方向性により、上位階層の階層化画像データにはアクセス不可能とすることを実現可能である。

【００３１】さらに、図４を参照して、各利用者が階層化画像データにアクセスする場合を説明する。まず、鍵kAを保持している最高解像度の画像データにアクセス可能な利用者Ａについて説明する。鍵kAを保持している利用者Ａは、図４の左側に示す画像ファイルフォーマットのヘッダの部分から、鍵kAを用いて復号し、鍵k0を得る。鍵k0を得た利用者Ａは、図３に示すように、鍵k0を用いて、暗号化階層化画像データencimg0を復号し、階層化画像データimg0を得ることが可能である。さらに、一方向性関数を用いて、鍵k0から鍵k1を得ることも可能である。以下同様に、鍵k1を用いて、暗号化階層化画像データencimg1を復号し階層化画像データimg1を得ることが可能であり、さらに、一方向性関数を用いて、鍵k1から鍵k2を得ることが可能である。さらに同様に、階層化画像データimg2も得ることが可能になり、画像データを復元（復号）することが可能となる。

【００３２】次に、鍵kBを保持している最低解像度の画像データにアクセス可能な利用者Ｂについて説明する。鍵kBを保持している利用者Ｂは、図４の右側に示す画像ファイルフォーマットのヘッダの部分から、鍵kBを用いて復号し、鍵k2を得る。鍵k2を得た利用者Ｂは、図３に示すように、鍵k2を用いて、暗号化階層化画像データencimg2を復号し、階層化画像データimg2を得ることが可能である。しかし、鍵の変換は一方向性関数による変換なので、鍵k2から鍵k1や鍵k0を得ることはできない。したがって、暗号化階層化画像データencimg1やencimg0を復号することもできず、階層化画像データimg1やimg0を得ることができない。つまり、鍵k2を保持する利用者は、鍵k2に対応する階層化画像データとそれ以下の階層化画像データしか得ることができない。これは、サムネイル画像データの利用のように最低解像度の画像データである最低階層化画像データだけの自由なアクセスの実現を容易に可能にする。つまり、本実施の形態は、最低階層化画像データの暗号化に用いた鍵を常に公開することにより、だれでも最低階層化画像データにアクセス可能とする一方で、鍵の一方向性により、上位階層の階層

10

化画像データにはアクセス不可能とすることを実現可能である。

【００３３】以上のように、暗号化部１０２は、各階層毎の鍵のうちの１つの鍵を暗号化し、暗号化された各階層の暗号化画像データencimg0～encimg2と共に出力する。利用者の画像処理装置は、階層構造をもつ画像データが各階層毎に異なる鍵で暗号化されている暗号化画像データ及び該階層毎の鍵のうちの１つの鍵を暗号化した鍵を入力する入力手段と、暗号化された鍵を復号し、該復号した鍵を用いて該鍵の階層に対応する階層及びその階層以下の階層の暗号化画像データを復号する復号手段とを有する。

【００３４】本実施の形態は、画像データを入力し、入力した画像データを階層化し、各階層化画像データをそれぞれ暗号化することにより、階層化画像データ毎にアクセス制御を実現する。つまり、暗号化を用いることにより、鍵に対応する階層化画像データだけを利用可能になり、階層化画像データ毎のアクセス制御を実現する。また、各階層毎の暗号化の鍵は、一方向性関数による変換に基づいて鍵を連鎖させることを特徴とする。言い換えると、特定の方向の鍵の連鎖だけを容易に計算可能であることである。さらに、鍵の連鎖の方向と階層化画像データの階層の上位から下位への方向とを一致させることにより、上位階層の暗号化の鍵から下位階層の暗号化の鍵を容易に求めることができるが、逆に下位階層の暗号化の鍵から上位階層の暗号化の鍵を求めることは困難、または不可能であることを実現する。つまり、上位の階層化画像データへアクセス可能であれば、下位の階層化画像データへアクセス可能であるが、逆に下位の階層化画像データへアクセス可能であっても、上位の階層化画像データへのアクセスは不可能であることを実現する。さらに、特定の階層化画像データに対応する鍵を利用者の鍵を用いて暗号化することにより、利用者への鍵の配送を容易にする。

【００３５】また、画像データの階層化は、解像度に基づいて階層化する方法や、重要度に基づいて階層化する方法や、SNR (Signal-to-Noise Ratio) に基づいて階層化する方法等あるが、特に限定しない。また、階層化画像データは、対応する階層に対する画像データとする方法や、隣接する階層化画像データとの差分データとする方法があるが、特に限定しない。

【００３６】さらにまた、サムネイル画像のように、最低解像度の画像データである最低階層化画像データを自由なアクセスとする方法において、最低階層化画像データの暗号化に用いた鍵を公開する方法を前述した。しかし、最低階層化画像データは暗号化を行わないことによっても、同様の機能を実現可能である。

【００３７】さらにまた、図５に示すような鍵の連鎖方法も考えられる。図５に示す鍵の連鎖方法では、乱数 Seed を一方向性関数で変換して、最高の階層化画像

データの暗号化の k0 を生成する。例えば、乱数 Seed を画像データの配信者と画像データに関連して生成することが考えられる。例えば、配信者毎に異なる秘密鍵（秘密情報）を Seed_Distributor、画像データを img とし、乱数 Seed を Seed = H (Seed_Distributor | img)とする。ただし、記号 | はデータの連結を表す。

【００３８】図 3 に示す鍵の連鎖方法では、複数の画像データを、異なるアクセス制御方法で配信する場合、各画像データ毎に鍵 k0 を管理する必要がある。しかし、図5 に示す鍵の連鎖方法であって、乱数 Seed を配信者毎の秘密鍵と画像データに依存させて生成する場合、配信者は秘密鍵を管理するだけで、複数の画像データを、異なるアクセス制御方法で配信することを可能にする。

【００３９】暗号アルゴリズムは、共通鍵暗号方式、公開鍵暗号方式に分類することができる。共通鍵暗号方式とは、共通の情報を鍵とし、鍵を送信者と受信者で秘密に共有し、それぞれ送信者側と受信者側でこの鍵を用いてメッセージを変換する方式である。秘密に同じ鍵を共有することから、秘密鍵暗号方式、対称鍵暗号方式、慣用暗号方式とも呼ばれる。共通鍵暗号方式としては、ＤＥＳ (Data Encryption Standard) やＡＥＳ (Advanced Encryption Standard) 等が知られている。また、公開鍵暗号方式とは、暗号化する鍵と復号する鍵が異なり、片方を公開することができる暗号方式である。公開する鍵を公開鍵、他方を秘密鍵と呼び、秘密鍵は秘密に保持する。公開鍵と秘密鍵は１対１に対応し、公開鍵で変換したメッセージはそれに対応する秘密鍵でだけ復号可能である。さらに、公開鍵から秘密鍵は分からないように設計されている。公開鍵暗号方式としては、ＲＳＡ暗号やＥｌＧａｍａｌ暗号等が知られている。さらに、公開鍵暗号方式を利用したシステムは、認証機関（以下、ＣＡという）と証明書と証明書失効リスト（以下、ＣＲＬという）を利用した公開鍵インフラストラクチャ（以下、ＰＫＩという）のもとで利用されることが多い。ＣＡによって作成された利用者の公開鍵に対する証明書と公開鍵を共に用いることにより、公開鍵の正当性を保証している。また、証明書の検証過程において、ＣＲＬを参照することにより、その証明書が取り消されていないかどうかの検査を可能にしている。

【００４０】本実施の形態における、画像データの配信者と利用者間の暗号方式は、前述の秘密鍵暗号方式や公開鍵暗号方式、さらにはＰＫＩをベースとした公開鍵暗号方式等が利用可能であり、鍵管理の厳密さ等によりそれぞれの方式を使い分けることが可能である。

【００４１】以上に説明したように、本実施の形態によれば、階層的な構造をもつ画像データであって、各階層毎の画像データに対して鍵を用いてアクセス制御を実現する場合において、鍵の管理を容易に行える方法を提供することができる。かつ、利用者への鍵の配送も容易に行える方法を提供することができる。なお、本実施の形態では画像データに限定されず、マルチメディアデータに適用することもできる。

【００４２】（第２の実施の形態）以下に、本発明の第2の実施の形態について説明する。第2の実施の形態は、JPEG2000画像符号化方式に適応させた場合について具体的に説明する。

【００４３】JPEG2000符号化方式について説明する。図6において、１は画像入力部、2は離散ウェーブレット変換部、3は量子化部、4はエントロピ符号化部、5は符号出力部、11は領域指定部である。

【００４４】まず、画像入力部１に対して符号化対象となる画像を構成する画素信号がラスタースキャン順に入力され、その出力は離散ウェーブレット変換部に入力される。以降の説明では画像信号はモノクロの多値画像を表現しているが、カラー画像等、複数の色成分を符号化するならば、ＲＧＢ各色成分、或いは輝度、色度成分を上記単色成分として圧縮すればよい。

【００４５】離散ウェーブレット変換部2は、入力した画像信号に対して2次元の離散ウェーブレット変換処理を行い、変換係数を計算して出力するものである。図7(a)は離散ウェーブレット変換部2の基本構成を表したものであり、入力された画像信号はメモリ201に記憶され、処理部202により順次読み出されて変換処理が行われ、再びメモリ201に書きこまれており、本実施の形態においては、処理部202における処理の構成は同図(b)に示すものとする。同図において、入力された画像信号は遅延素子およびダウンサンプラの組み合わせにより、偶数アドレスおよび奇数アドレスの信号に分離され、2つのフィルタｐおよびｕによりフィルタ処理が施される。同図sおよびdは、各々1次元の画像信号に対して1レベルの分解を行った際のローパス係数およびハイパス係数を表しており、次式により計算されるものとする。

【００４６】

$$d(n) = x(2*n + 1) - \mathrm{floor}((x(2*n) + x(2*n + 2))/2) \quad (式1)$$

$$s(n) = x(2*n) + \mathrm{floor}((d(n - 1) + d(n))/4) \quad (式2)$$

ただし、x(n)は変換対象となる画像信号である。

【００４７】以上の処理により、画像信号に対する1次元の離散ウェーブレット変換処理が行われる。2次元の離散ウェーブレット変換は、1次元の変換を画像の水平・垂直方向に対して順次行うものであり、その詳細は公知であるのでここでは説明を省略する。図7(c)は2次元の変換処理により得られる2レベルの変換係数群の構成例であり、画像信号は異なる周波数帯域の係数列HH1、HL1、LH1、…、LLに分解される。なお、以降の説明ではこれらの係数列をサブバンドと呼ぶ。各サブバンドの係数は後続の量子化部3に出力される。

【００４８】領域指定部11は符号化対象となる画像内

で、周囲部分と比較して高画質で復号化されるべき領域（ＲＯＩ：region of interesting）を決定し、対象画像を離散ウェーブレット変換した際にどの係数が指定領域に属しているかを示すマスク情報を生成する。図8(a)はマスク情報を生成する際の一例を示したものである。同図左側に示す様には所定の指示入力により画像内に星型の領域が指定された場合に、領域指定部11は、この指定領域を含む画像を離散ウェーブレット変換した際、該指定領域が各サブバンドに占める部分を計算する。

【００４９】このように計算されたマスク情報の例を図8(a)の右側に示す。この例においては、同図左側の画像に対し2レベルの離散ウェーブレット変換を施した際のマスク情報が図のように計算される。図中において星型の部分が指定領域であり、この領域内のマスク情報のビットは１、それ以外のマスク情報のビットは0となっている。これらマスク情報全体は2次元離散ウェーブレット変換による変換係数の構成と同じであるため、マスク情報内のビットを検査することで対応する位置の係数が指定領域内に属しているかどうかを識別することができる。このように生成されたマスク情報は量子化部3に出力される。

【００５０】さらに、領域指定部11は指定領域に対する画質を指定するパラメータを不図示の入力系から入力する。パラメータは指定領域に割り当てる圧縮率を表現する数値、あるいは画質を表す数値でもよい。領域指定部11はこのパラメータから、指定領域における係数に対するビットシフト量Bを計算し、マスクと共に量子化部3に出力する。

【００５１】量子化部3は、入力した係数を所定の量子化ステップにより量子化し、その量子化値に対するインデックスを出力する。ここで、量子化は次式により行われる。

q = sign (c) floor(abs(c) / Δ)　　(式3)

sign(c) = 1; c >= 0　　(式4)

sign(c) = -1; c < 0　　(式5)

ここで、cは量子化対象となる係数である。また、本実施の形態においてはΔの値として1を含むものとする。この場合実際に量子化は行われない。

【００５２】次に量子化部3は、領域指定部11から入力したマスクおよびシフト量Bに基づき、次式により量子化インデックスを変更する。

q' = q * 2^B; m = 1　　(式6)

q' = q　　; m = 0　　(式7)

ここで、mは当該量子化インデックスの位置におけるマスクの値である。以上の処理により、領域指定部11において指定された空間領域に属する量子化インデックスのみがBビット上方にシフトアップされる。

【００５３】図8(b)および(c)はこのシフトアップによる量子化インデックスの変化を示したものである。(b)は、あるサブバンドの量子化インデックス群であり、網掛けされた量子化インデックスにおけるマスクの値が1でシフト数Bが2の場合、シフト後の量子化インデックスは(c)のようになる。なお、このビットシフトにより生じる各空欄には図の様にビット0が補完される。このように変更された後の量子化インデックス群は後続のエントロピ符号化部4に出力される。

【００５４】なお、本実施の形態におけるマスクは、上記シフトアップ処理だけでなく、エントロピ符号化部4での符号化後に得られたデータから原画像を正確に復元する為に用いられるべき役割を担うが、本発明はこれに限らない。例えば、シフトアップの数Ｂをビットシフト処理の対象となる各量子化インデックスのビット数と同数（図8では４ビット）にすることを前提とすれば、マスクの情報は復号化側に送出せずともＲＯＩとそれ以外を復号化側は容易に判断でき、正確な原画像の復元は可能である。

【００５５】エントロピ符号化部4は入力した量子化インデックスをビットプレーンに分解し、ビットプレーンを単位に2値算術符号化を行ってコードストリームを出力する。図9はエントロピ符号化部4の動作を説明する図であり、この例においては4x4の大きさを持つサブバンド内の領域において非0の量子化インデックスが3個存在しており、それぞれ+13、-6、+3の値を持っている。エントロピ符号化部4はこの領域を走査して最大値Mを求め、次式により最大の量子化インデックスを表現するために必要なビット数Sを計算する。

S = ceil(log2(abs(M)))　　(式8)

ここでceil(x)はx以上の整数の中で最も小さい整数値を表す。

【００５６】図9においては、最大の係数値は13であるのでSは4であり、シーケンス中の16個の量子化インデックスは同図(b)に示すように4つのビットプレーンを単位として処理が行われる。最初にエントロピ符号化部4は最上位ビットプレーン(同図MSBで表す)の各ビットをエントロピ符号化（本実施の形態では2値算術符号化）し、ビットストリームとして出力する。次にビットプレーンを1レベル下げ、以下同様に対象ビットプレーンが最下位ビットプレーン（同図LSBで表す）に至るまで、ビットプレーン内の各ビットを符号化し符号出力部5に出力する。なお上記エントロピ符号化時において、各量子化インデックスの符号は、上位から下位へのビットプレーン走査において最初（最上位）に符号化されるべき非０ビットが検出されるとそのすぐ後に当該量子化インデックスの正負符号を示す１ビットを続けて２値算術符号化することとする。これにより、０以外の量子化インデックスの正負符号は効率良く符号化される。

【００５７】図10は、このようにして生成され出力される符号列の構成を表した概略図である。同図(a)は符号列の全体の構成を示したものであり、MHはメインヘッダ、THはタイルヘッダ、BSはビットストリームである。

15

メインヘッダMHは同図(b)に示すように、符号化対象となる画像のサイズ（水平および垂直方向の画素数）、画像を複数の矩形領域であるタイルに分割した際のサイズ、各色成分数を表すコンポーネント数、各成分の大きさ、ビット精度を表すコンポーネント情報から構成されている。なお、本実施の形態では画像はタイルに分割されていないので、タイルサイズと画像サイズは同じ値を取り、対象画像がモノクロの多値画像の場合コンポーネント数は１である。

【００５８】次にタイルヘッダTHの構成を図10(c)に示す。タイルヘッダTHには当該タイルのビットストリーム長とヘッダ長を含めたタイル長および当該タイルに対する符号化パラメータ、および指定領域を示すマスクと当該領域に属する係数に対するビットシフト数から構成される。符号化パラメータには離散ウェーブレット変換のレベル、フィルタの種別等が含まれている。本実施の形態におけるビットストリームの構成を同図(d)に示す。同図において、ビットストリームは各サブバンド毎にまとめられ、解像度の小さいサブバンドを先頭として順次解像度が高くなる順番に配置されている。さらに、各サブバンド内は上位ビットプレーンから下位ビットプレーンに向かい、ビットプレーンを単位として符号が配列されている。

【００５９】図11は、このようにして生成され出力される符号列の構成を表した概略図である。同図(a)は符号列の全体の構成を示したものであり、MHはメインヘッダ、THはタイルヘッダ、BSはビットストリームである。メインヘッダMHは同図(b)に示すように、符号化対象となる画像のサイズ（水平および垂直方向の画素数）、画像を複数の矩形領域であるタイルに分割した際のサイズ、各色成分数を表すコンポーネント数、各成分の大きさ、ビット精度を表すコンポーネント情報から構成されている。なお、本実施の形態では画像はタイルに分割されていないので、タイルサイズと画像サイズは同じ値を取り、対象画像がモノクロの多値画像の場合コンポーネント数は１である。

【００６０】次にタイルヘッダTHの構成を図11(c)に示す。タイルヘッダTHには当該タイルのビットストリーム長とヘッダ長を含めたタイル長および当該タイルに対する符号化パラメータ、および指定領域を示すマスクと当該領域に属する係数に対するビットシフト数から構成される。符号化パラメータには離散ウェーブレット変換のレベル、フィルタの種別等が含まれている。本実施の形態におけるビットストリームの構成を同図(d)に示す。同図において、ビットストリームはビットプレーンを単位としてまとめられ、上位ビットプレーンから下位ビットプレーンに向かう形で配置されている。各ビットプレーンには、各サブバンドにおける量子化インデックスの当該ビットプレーンを符号化した結果が順次サブバンド単位で配置されている。図においてSは最大の量子化インデックスを表現するために必要なビット数である。このようにして生成された符号列は、符号出力部5に出力される。

16

【００６１】上述した実施の形態符号化装置においてよれば、符号化対象となる画像全体の圧縮率は量子化ステップΔを変更することにより制御することが可能である。また別の方法として本実施の形態では、または，エントロピ符号化部4において符号化するビットプレーンの下位ビットを必要な圧縮率に応じて制限（廃棄）することも可能であるとしてもよい。この場合には、全てのビットプレーンは符号化されず上位ビットプレーンから所望の圧縮率に応じた数のビットプレーンまでが符号化され、最終的な符号列に含まれる。

【００６２】上記下位ビットプレーンを制限する機能を利用すると、図8に示した指定領域に相当するビットのみが多く符号列に含まれることになる。即ち、上記指定領域のみ低圧縮率で高画質な画像として符号化することが可能となる。

【００６３】本実施の形態における画像データのひとつは、図10に示された符号列である。図10に示された符号列は、図10(a)に示されるように、タイル単位、つまりタイルヘッダTHnとビットストリームBSnの組の単位で符号化されているとみなすことが可能である。つまり、TH0とBS0の組、TH1とBS1の組のように、タイルヘッダとビットストリームの組をそれぞれ階層化画像データとみなすことが可能である。これらのTH0とBS0の組を第1の実施の形態の階層化画像データimg0、TH1とBS1の組を階層化画像データimg1、THnとBSnを階層化画像データimgnとみなすことで、第1の実施の形態で説明した暗号化方式が適応可能であり、適応例を図12に示す。図12(a)に示すように、階層化画像データTH0とBS0の組は、鍵k0で暗号化され、暗号化階層化画像データencimg0となる。階層化画像データTH1とBS1の組は、鍵k0から変換された鍵k1で暗号化され、暗号化階層化画像データencimg1となる。以下同様に、階層化画像データTH2とBS2、TH3とBS3も暗号化される。最終的に、図10(a)に示された符号化列は、図12(b)のように暗号化される。

【００６４】また、図10に示された符号化列に含まれるビットストリームは、図10(d)に示されるようにサブバンド単位で符号化されているとみなすことが可能である。つまり、LL、HL2、LH2等のサブバンド符号化データをそれぞれ階層化画像データとみなすことが可能であり、第1の実施の形態の適応例を図13に示す。図13(a)に示すように、階層化画像データLLは鍵k0で暗号化され、暗号化階層化画像データencimg0となる。階層化画像データHL2は、鍵k0から変換された鍵k1で暗号化され、暗号化階層化画像データencimg1となる。以下同様に、階層化画像データLH2、HH2も暗号化される。最終的に、図10(d)に示されたサブバンド単位の符号列は、図13(b)のように暗号化される。

17

【００６５】さらに、図10に示された符号化列に含まれるサブバンド符号化データは、図10(d)に示されるようにビットプレーン単位で符号化されているとみなすことが可能である。つまり、ビットプレーン単位のデータBit Plane S-1、Bit Plane S-2をそれぞれ階層化画像データとみなすことが可能であり、上記タイル単位の符号化やサブバンド単位の符号化と同様に、第1の実施の形態を適応することが可能である。

【００６６】図11に示した符号列に対しても、前述の図10に示した符号列と同様に第1の実施の形態を適応することが可能である。つまり、第1に図11(a)に対応して各タイル単位のデータを階層化画像データとみなす場合、第2に図11(d)に対応して各ビットプレーン単位のデータを階層化画像データとみなす場合、第3に図11(d)に対応して各サブバンド単位のデータを階層化画像データとみなす場合がそれぞれ可能であり、それぞれに対して、第1の実施の形態を適応することが可能である。

【００６７】図10の符号化列を対象にした場合、先に述べたように、タイル単位、サブバンド単位、ビットプレーン単位と3つのパラメータによる階層化画像データの生成方法がある。本発明は、単一のパラメータによる階層化画像データの暗号化も可能であるが、タイル単位の階層化画像データに対する暗号化とサブバンド単位の階層化画像データに対する暗号化とビットプレーン探知の階層化画像データに対する暗号化を同時に行うことも可能である。

【００６８】さらに、各パラメータによる階層化画像データの暗号化に用いる鍵は、各パラメータによる階層化画像データ毎に独立の鍵の連鎖を利用することも可能であるし、単一の鍵の連鎖を利用することも可能である。

【００６９】上記の方法における、パケットの集合である画像データの符号列と暗号鍵の対応を図14に示す。暗号対象となるパケットは、符号列をタイル単位やサブバンド単位やビットプレーン単位等による一般的なデータパケットを表しており、特定の単位に限定していない。上述の方法は、図14に示すように、符号化列中のパケットの順序と鍵の連鎖の順序が同一の方向である。鍵を保持するユーザは、その鍵とその鍵から変換して得られる鍵だけが利用可能である。つまり、図14において、key1を保持するユーザAは、key2、key3、...、keynを利用可能であるが、key0を得ることはできない。つまり、ユーザAはPacket1、Packet2、...、Packetnを利用可能となり、Packet0を利用することができず、JPEG2000符号列を正しく復号できない可能性が生じる。

【００７０】これに対して、図15に示す画像データの符号列と暗号化鍵の対応を取ることで、上述の問題を対応することが可能である。つまり、符号列の最初に現れるパケット程、低い階層化データとして扱う方法である。上述の方法と同じであるので、詳細の説明は省略する。

【００７１】以上に説明したように、第2の実施の形態

18

によれば、JPEG2000画像符号化方式がもつ階層的な画像データに適応に対して鍵を用いてアクセス制御を実現する場合において、鍵の管理を容易に行える方法を提供することができる。

【００７２】（本発明の他の実施の形態）本実施形態は、コンピュータがプログラムを実行することによって実現することができる。また、プログラムをコンピュータに供給するための手段、例えばかかるプログラムを記録したＣＤ－ＲＯＭ等のコンピュータ読み取り可能な記録媒体又はかかるプログラムを伝送するインターネット等の伝送媒体も本発明の実施形態として適用することができる。また、上記のプログラムを記録したコンピュータ読み取り可能な記録媒体等のプログラムプロダクトも本発明の実施形態として適用することができる。上記のプログラム、記録媒体、伝送媒体及びプログラムプロダクトは、本発明の範疇に含まれる。記録媒体としては、例えばフレキシブルディスク、ハードディスク、光ディスク、光磁気ディスク、ＣＤ－ＲＯＭ、磁気テープ、不揮発性のメモリカード、ＲＯＭ等を用いることができる。

【００７３】なお、上記実施形態は、何れも本発明を実施するにあたっての具体化の例を示したものに過ぎず、これらによって本発明の技術的範囲が限定的に解釈されてはならないものである。すなわち、本発明はその技術思想、またはその主要な特徴から逸脱することなく、様々な形で実施することができる。

【００７４】

【発明の効果】以上説明したように、各階層毎のデータに対して各階層毎の鍵を用いて暗号化する際に、特定の鍵を基に各階層毎に異なる鍵を生成するので、鍵の管理を容易に行うことができる。また、暗号化されたデータと共に暗号化された鍵を利用者に供給することにより、利用者への鍵の配送も容易に行うことができる。

【図面の簡単な説明】

【図１】本発明の実施の形態における画像アクセス制御装置の構成を示した構成図である。

【図２】本発明の第１の実施の形態における鍵変換部の構成を示した構成図である。

【図３】本発明の第１の実施の形態における画像データと暗号化鍵の第１の対応を示した図である。

【図４】本発明の第１の実施の形態における画像ファイルフォーマットを示した図である。

【図５】本発明の第１の実施の形態における画像データと暗号化鍵の第２の対応を示した図である。

【図６】本発明の第２の実施の形態におけるJPEG2000画像符号化装置の構成を示した図である。

【図７】本発明の第２の実施の形態における離散ウェーブレット変換部の基本構成を示した図である。

【図８】本発明の第２の実施の形態における領域指定部の処理を示した図である。

19

【図９】本発明の第２の実施の形態におけるエントロピ符号化部の動作を説明する図である。

【図１０】本発明の第２の実施の形態における生成され出力される符号列の構成を表した概略図である。

【図１１】本発明の第２の実施の形態における生成され出力される他の符号列の構成を表した概略図である。

【図１２】本発明の第２の実施の形態におけるタイルヘッダとビットストリームを階層化画像データとした暗号化方式を示した図である。

【図１３】本発明の第２の実施の形態におけるサブバンド符号化データを階層化画像データとした暗号化方式を示した図である。

【図１４】本発明の第２の実施の形態におけるパケットの集合である画像データの符号列と暗号鍵の対応を示した図である。

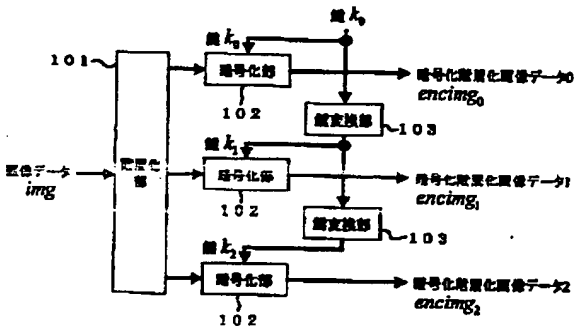
20

【図１５】本発明の第２の実施の形態におけるパケットの集合である画像データの符号列と暗号鍵の他の対応を示した図である。

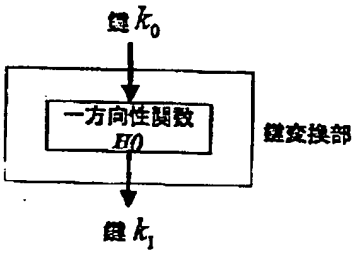
【符号の説明】

1　画像入力部
2　離散ウェーブレット変換部
3　量子化部
4　エントロピ符号化部
5　符号出力部
１１　領域指定部
１０１　階層化部
１０２　暗号化部
１０３　鍵変換部
２０１　メモリ
２０２　処理部

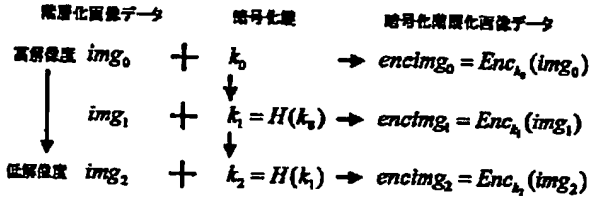
【図１】



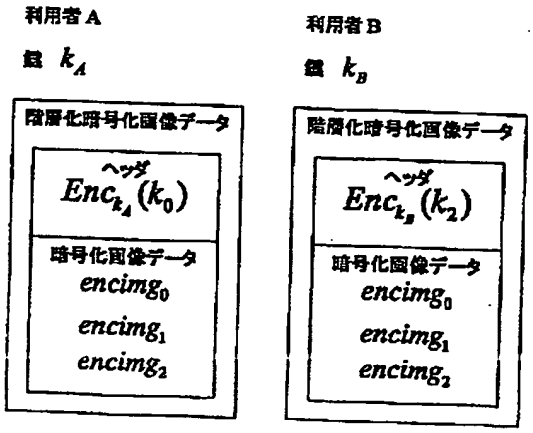
【図２】



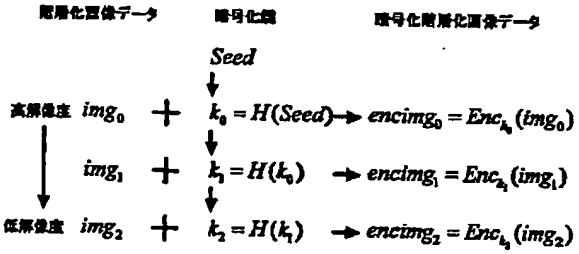
【図３】



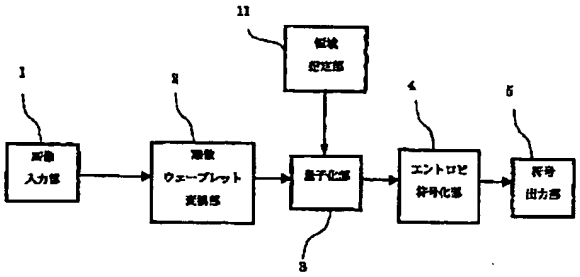
【図４】



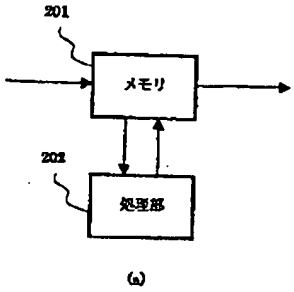
【図５】



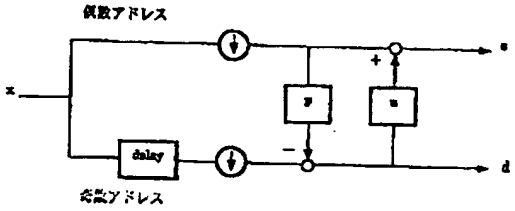
【図６】



【図７】

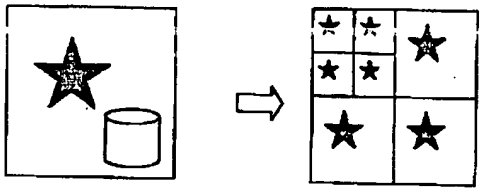


(a)



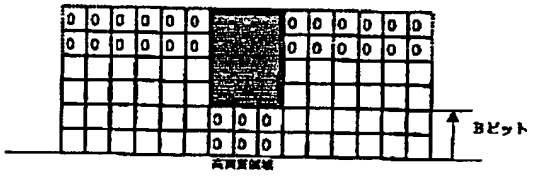
(b)

【図８】

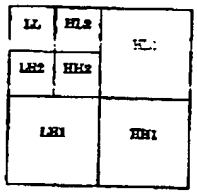


(a)

(b)

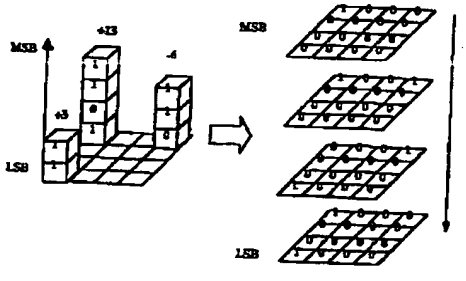


(c)



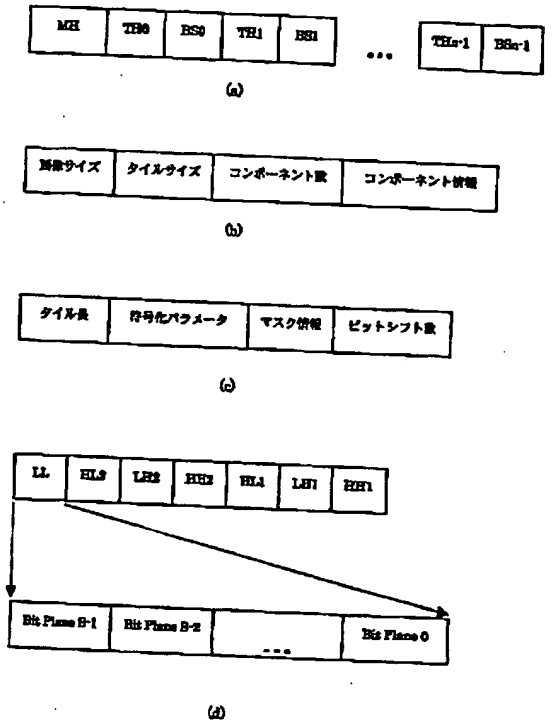
(c)

【図９】

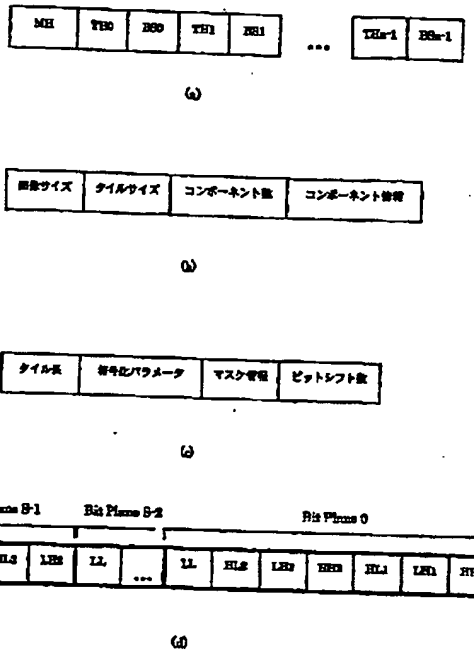


(a)　　(b)

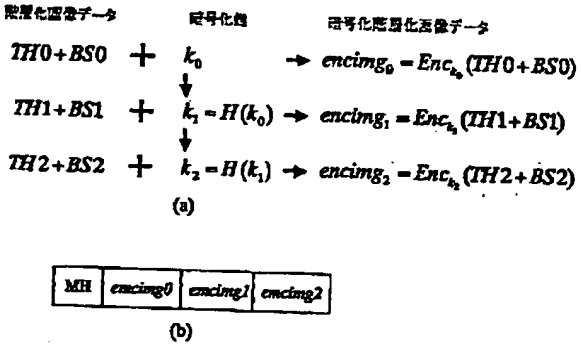
【図１０】



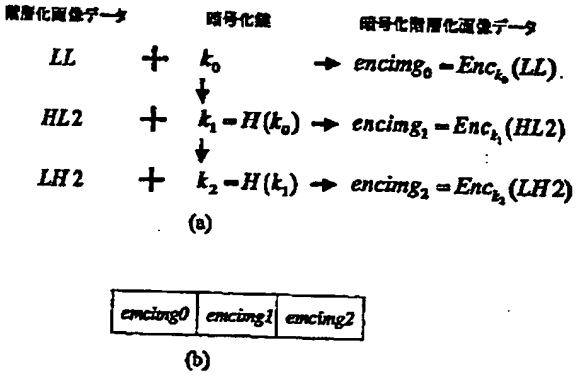
【図１１】



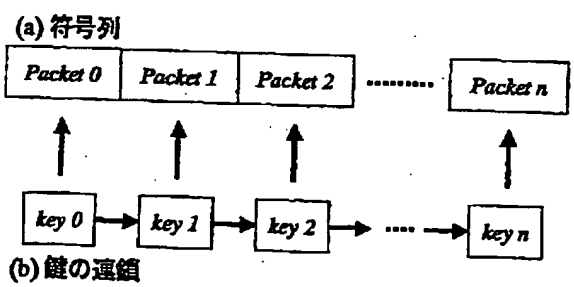
【図１２】



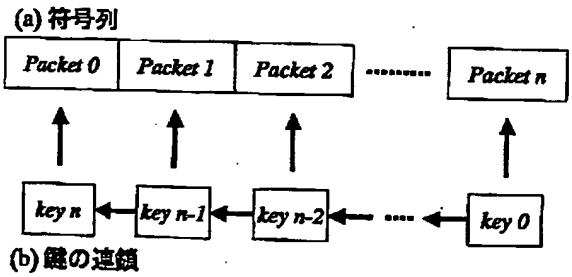
【図１３】



【図１４】



【図１５】



フロントページの続き

(72)発明者　林　淳一
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

(72)発明者　岩村　恵市
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内

Ｆターム(参考)　5C064 BA01 BB02 BC16 BD09
5J104 AA16 EA04 EA06 JA01 NA02
NA11